(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
11. August 2005 (11.08.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/074310 A1

(51) Internationale Patentklassifikation[7]: H04Q 7/32, H04M 17/00

(21) Internationales Aktenzeichen: PCT/EP2005/050295

(22) Internationales Anmeldedatum:
24. Januar 2005 (24.01.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
04100328.6 29. Januar 2004 (29.01.2004) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SWISSCOM MOBILE AG** [CH/CH]; Schwarztorstrasse 61, CH-3050 Bern (CH).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **AEBI, Paul** [CH/CH]; Urtenenweg 7, CH-3303 Münchringen (CH).

(74) Anwalt: **BOVARD AG**; Optingenstrasse 16, CH-3000 Bern 25 (CH).

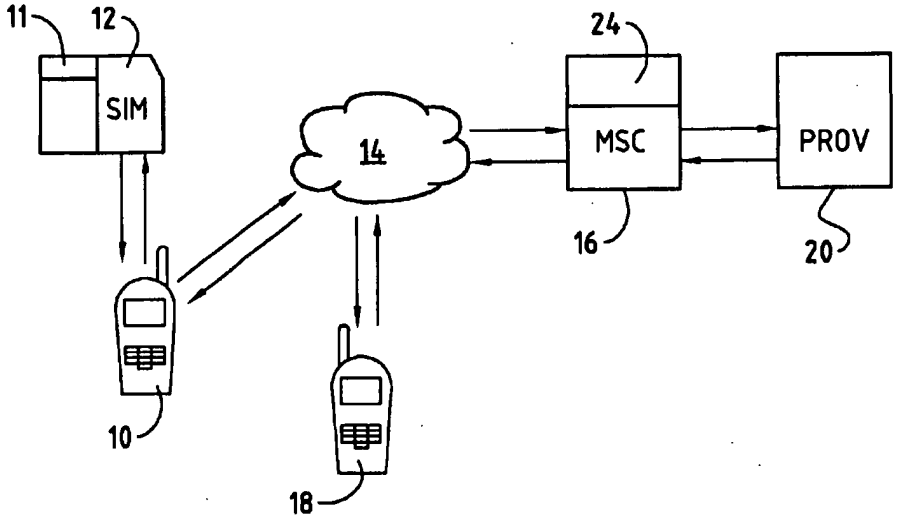
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND SYSTEM FOR TRANSMITTING USEFUL DATA BETWEEN TELECOMMUNICATION DEVICES

(54) Bezeichnung: VERFAHREN UND SYSTEM FÜR DIE ÜBERTRAGUNG VON NUTZDATEN ZWISCHEN TELEKOMMUNIKATIONSGERÄTEN



(57) Abstract: The invention relates to a method and system for transmitting useful data between telecommunication terminals (10,18), wherein pre-paid access data comprising a first digital key and control data, is stored in a memory module (11) of a telecommunication terminal (10), wherein a second digital key is stored on one or several control units (16) of the telecommunication network (14). A validity criterion is determined on the basis of control data and the useful data of the first telecommunication terminal is coded by means of a first key, in so far as the validity criterion is met. The coded useful data is transmitted to the control unit (16), is decoded by means of the second digital key and is transmitted to another telecommunication terminal (18).

[Fortsetzung auf der nächsten Seite]

WO 2005/074310 A1

EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärung gemäß Regel 4.17:

— *Erfindererklärung (Regel 4.17 Ziffer iv) nur für US*

Veröffentlicht:

— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren und System zur Übertragung von Nutzdaten zwischen Telekommunikationsgeräten (10,18), wobei vorausbe-zahlte Zugangsdaten, welche einen ersten digitalen Schlüssel und Kontrolldaten umfassen, in einem Speichermodul (11) eines Telekommunikationsgeräts (10) abgespeichert werden, wobei ein zweiter digitaler Schlüssel auf einer oder mehreren Steuereinheiten (16) des Telekommunikationsnetzwerks (14) abgespeichert wird, wobei basierend auf Kontrolldaten ein Gültigkeitskriterium ermittelt wird und Nutzdaten des ersten Telekommunikationsgeräts mittels des ersten Schlüssels codiert werden, solange das Gültigkeitskriterium erfüllt ist, und wobei die codierte Nutzdaten an die Steuereinheit (16) übermittelt, mittels des zweiten digitalen Schlüssels decodiert und an ein weiteres Telekommunikationsgerät (18) übermittelt werden.

Verfahren und System für die Übertragung von Nutzdaten zwischen Telekommunikationsgeräten

Technisches Gebiet

Die vorliegende Erfindung betrifft ein Verfahren und System zur Übertragung von Nutzdaten zwischen Telekommunikationsgeräten. Die Erfindung bezieht sich insbesondere auf ein Verfahren und System einer auf vorausbezahlten Zugangsdaten basierten Übertragung von Nutzdaten zwischen Telekommunikationsgeräten.

Stand der Technik

Ein Dienstanbieter muss für die Übermittlung von Nutzdaten zwischen Telekommunikationsgeräten eine Netzwerkinfrastruktur aufbauen und betreiben. Es ist bekannt, Mobiltelefone mit vorausbezahlten Gebühren zu betreiben, d.h. im so genannten Prepaid-Modus. Bei dieser Betriebsart, welche in der Regel kein Abonnement bei einem bestimmten Provider benötigt, führt der Provider ein Gebührenkonto, das durch die Anschlusskennung des Mobiltelefons und in der Regel durch weitere Kennungen, die in aller Regel verschlüsselt sind, identifiziert wird. Die Kennungen sind beim Provider und/oder im Chip der SIM-Karte (Subscriber Identity Module) gespeichert, die sich im Mobiltelefon befinden muss, damit dieses für Telekommunikationen betrieben werden kann. Solche zusätzlichen Kennungen sind beispielsweise Zertifikate, die die Berechtigung des Mobiltelefon-Nutzers bestätigen und die bei einem Verbindungsaufbau überprüft werden. Falls das Gebührenkonto beim Provider in Echtzeit nachgeführt werden soll, dann muss während einem Telefongespräch beispielsweise im Sekundentakt eine Nachführung gemäss dem für das Telefongespräch gültigen Tarif erfolgen. Dies im Gegensatz zu einem Gebührenkonto bei welchem Gespräche im Nachhinein abgerechnet werden und deshalb die Nachführung des Gebührenkontos beispielsweise nur bei Gesprächsende erfolgen muss. Mobiltelefone im Prepaid-Modus können zu einem sehr hohen technischem Aufwand für die Nachführung von Gebührenkontos führen.

In der Offenlegungsschrift DE 100 39 434 A1 wird ein Verfahren zur Nachführung eines Zählers eines Endgeräts zur Gebührenabrechnung be-

schrieben. Eine Kontrolleinrichtung des Dienstanbieters sendet Steuerbefehle an einen Datenträger eines Endgeräts, wobei der Zähler entsprechend der Steuerbefehle während einem Telefongespräch durch das Endgerät in einem bestimmten Takt nachgeführt wird, und wobei die Nachführung des Zählers gegenüber dem Dienstanbieter bestätigbar ist. Ein Nachteil dieses Verfahrens ist es, dass die Nachführung des Zählers des Endgeräts durch den Dienstanbieter nur durch entsprechende Steuerbefehle überprüfbar ist. Es ist weiter ein Nachteil, dass für die Überprüfung des Zählers beim Dienstanbieter ein Abbild des Zählers (Konto des Benutzers) vorhanden sein muss.

Aus der internationalen Patentanmeldung WO 03/079713 ist ein Verfahren zum Betrieb von Mobilfunk-Endgeräten bekannt, bei dem WIM-Funktionalitäten (Wireless Identification Module) bereitgestellt und abgerechnet werden, dadurch gekennzeichnet, dass die WIM intern, d.h. im Endgerät bzw. dem dort befindlichen SIM-Identifikationsmodul, realisiert wird. Dabei wird intern jede vom Teilnehmer initiierte Signatur gezählt, und zwar von einem Ausgangszustand zurück, bis die voreingestellte Anzahl von Signaturen erreicht ist. Dann wird das Gerät bis zu einer erneuten Signaturzahl-Aufladung gesperrt. Nachteilig an diesem Verfahren ist es, dass die Behandlung der Signatur, d.h. der digitalen Daten der Zugangsrechte, mit Ausnahme der Sperr- und Freischaltungen keine Datenverarbeitung vorsieht und nur eine einfache Zählfunktion ausübt, ohne Überprüfung des Volumens der mit einer einzelnen Signatur zu versehenden digitalen Daten, so dass eine Führung von Nutzkonten beim Betreiber (Provider) immer noch erforderlich ist, wobei bei einem Telefongespräch stets eine Verbindung vom MSC (Mobile Switching Center) zum Provider aufgebaut und unterhalten werden muss. Bei diesem Schritt können Fehler auftreten, z.B. infolge Übermittlungsstörungen, so dass die Nutzkonten verfälscht werden können. Es ist weiter ein Nachteil, dass auch keine Volumenbasierte Abrechnung möglich ist.

Offenbarung der Erfindung

Es ist eine Aufgabe der Erfindung, ein neues Verfahren und System zur Übertragung von Nutzdaten zwischen Telekommunikationsgeräten vorzuschlagen, welche die oben genannten Nachteile des Standes der Technik nicht aufweisen. Insbesondere soll ein automatisiertes, einfaches und rationelles

Verfahren und System vorgeschlagen werden, das ganz allgemein die Sicherheit der Abrechnung der Nutzdaten sowie auch die Zuverlässigkeit der Behandlung der digitalen Daten der Zugangsrechte verbessert und zudem beschleunigt.

Gemäss der vorliegenden Erfindung wird dieses Ziel insbesondere durch die Elemente der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

Insbesondere werden diese Ziele durch die Erfindung dadurch erreicht, dass ein Zentralmodul vorausbezahlte Zugangsdaten erzeugt, wobei die vorausbezahlten Zugangsdaten einen ersten digitalen Schlüssel und Kontrolldaten umfassen, und wobei die vorausbezahlten Zugangsdaten in einem Speichermodul des ersten Telekommunikationsgeräts abgespeichert werden, dass das Zentralmodul einen dem ersten digitalen Schlüssel zugeordneten zweiten digitalen Schlüssel erzeugt, wobei der zweite digitale Schlüssel auf einer oder mehreren Steuereinheiten des Telekommunikationsnetzwerks abgespeichert wird, dass das erste Telekommunikationsgerät basierend auf Kontrolldaten der vorausbezahlten Zugangsdaten ein Gültigkeitskriterium ermittelt und Nutzdaten des ersten Telekommunikationsgeräts mittels des ersten Schlüssels codiert, solange das Gültigkeitskriterium erfüllt ist, und dass das erste Telekommunikationsgerät codierte Nutzdaten an die Steuereinheit übermittelt, wobei die Steuereinheit mittels des zweiten digitalen Schlüssels überprüft, dass die codierten Nutzdaten mit dem ersten digitalen Schlüssel codiert sind, wobei die Steuereinheit bei einer erfolgreichen Überprüfung die codierten Nutzdaten decodiert, und wobei die Steuereinheit die decodierten Nutzdaten an das zweite Telekommunikationsgerät übermittelt. Die Nutzdaten können beispielsweise aus digitalisierten Sprachsignalen oder aus irgendwelchen anderen Daten bestehen. Die erfindungsgemässe Lösung hat u.a. den Vorteil, dass für die Abrechnung von im Prepaid-Modus getätigte Gespräche eines Mobilfunkgeräts kein Gebührenkonto einer Zentraleinheit des Dienstanbieters nachgeführt werden muss, dass insbesondere eine Volumenbasierte Abrechnung ermöglicht wird, und dass der Dienstanbieter zu jedem Zeitpunkt über die Berechtigung zur Führung eines Gesprächs informiert bleibt.

In einer Ausführungsvariante werden die im Speichermodul des ersten Telekommunikationsgeräts abgespeicherten vorausbezahlten Zugangsdaten bei der Codierung von Nutzdaten modifiziert und/oder gelöscht. Diese Ausführungsvariante hat u.a. den Vorteil, dass beispielsweise Gespräche mit einem Mobilfunkgerät entsprechend der Dauer oder der Datenmenge abgerechnet werden können.

In einer anderen Ausführungsvariante umfassen die im Speichermodul des ersten Telekommunikationsgeräts abgespeicherten vorausbezahlten Zugangsdaten einen Geldbetragswert, wobei dieser Geldbetragswert bei der Codierung von Nutzdaten modifiziert und/oder gelöscht wird. Diese Ausführungsvariante hat u.a. den Vorteil, dass dem Benutzer der Wert der gespeicherten vorausbezahlten Zugangsdaten einfach anzeigbar ist oder dass gespeicherte vorausbezahlte Zugangsdaten einfach zwischen Telekommunikationsgeräten transferierbar sind.

In einer anderen Ausführungsvariante werden die vorausbezahlten Zugangsdaten auf einem SIM-Modul des ersten Telekommunikationsgeräts abgespeichert. Diese Ausführungsvariante hat u.a. den Vorteil, dass die vorausbezahlten Zugangsdaten in einem durch einen Dienstanbieter kontrollierbaren Speicherbereich abspeicherbar sind oder dass durch ein Umstecken des SIM-Moduls vorausbezahlte Zugangsdaten leicht zwischen Telekommunikationsgeräten transferierbar sind.

In einer Ausführungsvariante umfasst die Codierung der Nutzdaten eine digitale Verschlüsselung und/oder digitale Signierung und die Decodierung der Nutzdaten eine entsprechende digitale Entschlüsselung und/oder Verifikation einer digitalen Signatur. Eine solche Ausführungsvariante hat u.a. den Vorteil, dass weit verbreitete Module von Telekommunikationsgeräten und Steuereinheiten für die Codierung und Decodierung von Nutzdaten verwendbar sind.

In einer Ausführungsvariante umfassen die vorausbezahlten Zugangsdaten eine Berechtigung für die Codierung einer bestimmbaren Nutzdatenmenge, wobei die vorausbezahlten Zugangsdaten gelöscht werden, sobald

die Codierung der bestimmbaren Nutzdatenmenge abgeschlossen ist. Diese Ausführungsvariante hat u.a. den Vorteil, dass vorausbezahlte Zugangsdaten auf dem ersten Telekommunikationsgerät sehr effizient verwaltbar sind.

In einer Ausführungsvariante sind mehrere Blöcke mit vorausbezahlten Zugangsdaten im Speichermodul des ersten Telekommunikationsgeräts abspeicherbar. Diese Ausführungsvariante hat u.a. den Vorteil, dass bei einem Fehlschlagen des Gültigkeitskriteriums für die Codierung von Nutzdaten sehr effizient auf einen nächsten Block mit vorausbezahlten Zugangsdaten umgeschaltet werden kann.

In einer Ausführungsvariante umfassen die Kontrolldaten mehrere Blöcke, wobei für jeden Block die Ermittlung eines Gültigkeitskriteriums sowie die Modifikation oder Löschung des entsprechenden Blocks von Kontrolldaten durchführbar ist. Diese Ausführungsvariante hat u.a. den Vorteil, dass der erste digitale Schlüssel mehrfach verwendbar ist und der Speicherbedarf für die Speicherung der vorausbezahlten Zugangsdaten reduzierbar ist.

An dieser Stelle soll festgehalten werden, dass sich die vorliegende Erfindung neben dem erfindungsgemässen Verfahren auch auf ein System zur Ausführung dieses Verfahrens bezieht. Ferner beschränkt es sich nicht auf das genannte System und Verfahren, sondern bezieht sich ebenso auf ein Computerprogrammprodukt zur Realisierung des erfindungsgemässen Verfahrens.

Kurze Beschreibung der Zeichnungen

Nachfolgend werden Ausführungsvarianten der vorliegenden Erfindung anhand von Beispielen beschrieben. Die Beispiele der Ausführungen werden durch folgende beigelegte Figuren illustriert:

Figur 1 zeigt schematisch ein Prepaid-System des Standes der Technik.

Figur 2 illustriert schematisch ein System zur Ausführung des erfindungsgemässen Verfahrens.

Ausführungsformen der Erfindung

Figur 1 illustriert schematisch eine Architektur des Standes der Technik. In diesem Ausführungsbeispiel ist ein Mobiltelefongerät 10 dargestellt, in das eine Prepaid-SIM-Karte 12 einsetzbar ist. Über Funk lässt sich das Telefongerät 10 mit dem Mobilfunknetzwerk 14 verbinden. Das Kommunikationsnetz 14 umfasst beispielsweise ein GSM- (Global System for Mobile communication) oder ein UMTS-Netz (Universal Mobile Telephone System), oder ein satellitenbasiertes Mobilfunknetz, und/oder ein oder mehrere Festnetze, beispielsweise das öffentlich geschaltete Telefonnetz, das weltweite Internet oder ein geeignetes LAN (Local Area Network) oder WAN (Wide Area Network). Insbesondere kann es auch ISDN- und XDSL-Verbindungen umfassen. Dieses Netzwerk steht wiederum in Datenaustausch-Verbindung mit dem MSC (Mobile Switching Center) 16. Das Netzwerk und das MSC sind nach dem GSM-Standard (Global System for Mobile Communication) aufgebaut. Der gewünschte Telefonteilnehmer, der mit dem Mobiltelefon 10 angewählt werden soll, ist mit 18 bezeichnet. Bei diesem Gerät kann es sich um ein Festtelefon, ein Mobiltelefon oder um eine beliebige andere Telekommunikations-Einheit handeln (z.B. auch ein Fax).

Mit dem MSC steht ein Provider 20 (PROV) mit einer Provider-Datenbank 22 in Verbindung, da ja für die Gebühren der zu führenden Prepaid-Konten eine entsprechende Kontenstelle vorhanden sein muss. Diese befindet sich in der Datenbank 22. Die Daten des in Frage stehenden Prepaid-Kontos werden in der Datenbank 22 gespeichert und dort beim Aktivieren des Teilnehmerkontos nachgeführt.

Der Ablauf des Verbindungsaufbaus, der auch die Prüfung der Berechtigung (Signatur) und die Kontenüberwachung und -führung umfasst, ist allgemein bekannt und soll nicht in Einzelheiten beschrieben werden.

Fig. 2 zeigt nun schematisch den Aufbau eines erfindungsgemässen Systems. Elemente und Bestandteile, die in Fig. 1 und 2 die gleichen bzw. einander ähnlich sind, tragen die gleichen Bezugszeichen.

Auf der SIM-Karte 12 befindet sich ein zusätzliches Speichermodul 11 für die Abspeicherung von vorausbezahlten Zugangsdaten, wie z.B. DRM-Daten (DRM: Digital Rights Management), beispielsweise in verschlüsselter Form, bevorzugt in digital verschlüsselter Form. Dabei ist das Speichermodul 11 vorzugsweise physikalisch vom übrigen Speicherfeld des SIM-Moduls 12 getrennt. Beim Aufladen der SIM-Karte, beispielsweise von einer für diesen Zweck eingerichteten Aufladekarte oder aber von einer Bankkreditkarte, werden die vorausbezahlten Zugangsdaten beispielsweise über den Provider 20 und den Server 16 an die SIM-Karte 12 übermittelt und dort im Speichermodul 11 abgespeichert. Zugleich wird auf einer Steuereinheit, beispielsweise in einem Speichermodul 24 eines MSC (Mobile Switching Center), ein zweiter digitaler Schlüssel, welcher dem ersten digitalen Schlüssel wie nachfolgend beschrieben zugeordnet ist, abgespeichert. Das SIM-Modul erteilt dem Mobiltelefon das Recht, Gespräche unter bestimmten Nutzungsbedingungen (z.B. Ziel, Dauer) mit den vorausbezahlten Zugangsdaten zu führen, d.h. die Nutzdaten bzw. die Gesprächsdaten mittels einem ersten digitalen Schlüssels der vorausbezahlten Zugangsdaten zu codieren, zu verschlüsseln und/oder zu signieren. Die Nutzdaten können z.B. speicherbar sein (beispielsweise SMS (Short Message Service), MMS (Multimedia Message Service), MP3 der Moving Picture Experts Group (MPEG) etc.) und/oder nicht speicherbar, wie z.B. ein Datastream und/oder Voice Data etc.

Beim Telefonieren mit dem Gerät 10 werden die Tondaten und/oder Nutzdaten codiert, d.h. mit dem ersten digitalen Schlüssel verschlüsselt und/oder signiert und/oder andersartig geeignet kombiniert, und an das MSC 16 übertragen. Auf dem MSC 16 wird mittels eines zweiten digitalen Schlüssels überprüft, ob die codierten Daten mit dem ersten digitalen Schlüssel codiert sind. Ist diese Überprüfung erfolgreich, dann werden die codierten Nutzdaten decodiert, also beispielsweise entschlüsselt und/oder es wird eine Signatur entfernt. Die decodierten Nutzdaten werden anschliessend an ein zweites Telekommunikationsgerät übermittelt für welches der Benutzer des ersten Telekommunikationsgeräts die Übertragung wünscht oder eingestellt hat. Während der Übermittlung werden die anfallenden Gebühren, welche wie üblich eine Funktion mehrerer Parameter (Dauer, Entfernung, Tageszeit, Art des Gerätes 18) sind, von Kontrolldaten der vorausbezahlten Zugangsdaten abgebucht.

Wenn der vorausbezahlte Betrag, dessen Daten auf dem SIM-Modul gespeichert sind, aufgebraucht ist, werden die vorausbezahlten Zugangsdaten annulliert und die Übertragung wird abgebrochen, eventuell nach einer entsprechenden Warnung. Die Warnungsdaten sind beispielsweise ebenfalls in den Kontrolldaten der vorausbezahlten Zugangsdaten gespeichert und werden von dort abgerufen. Das Speichermodul der SIM-Karte kann aber auch so eingerichtet sein, dass gleichzeitig mehrere Blöcke mit vorausbezahlten Zugangsdaten abspeicherbar sind. In diesem Fall kann nachdem ein erster Block mit vorausbezahlten Zugangsdaten annulliert wurde zuerst überprüft werden, ob ein weiterer Block mit vorausbezahlten Zugangsdaten verfügbar ist, wobei ein solcher Block für die Fortsetzung einer bestehenden Gesprächsverbindung verwendbar ist.

Vor erneutem Aufladen des Datenspeichers mit vorausbezahlten Zugangsdaten ist keine weitere Übermittlung oder aber nur bestimmte, begrenzte Übermittlungen (Notruf, Aufladenummern) von Nutzdaten zu anderen Telekommunikationsgeräten möglich.

Aus Obigem geht hervor, dass die Erfindung eine Möglichkeit schafft, das Telefonkonto beim Prepaid-Betrieb direkt auf dem Mobiltelefon zu führen und den Umweg über ein Provider-Konto zu vermeiden. Es ist dem Fachmann klar, dass der Erfindungsgedanke und das darauf beruhende, hierin beanspruchte Verfahren auch mit anderen Bauelementen und Systemeinheiten verwirklicht werden kann.

Ansprüche

1. Verfahren zur Übertragung von Nutzdaten zwischen einem ersten Telekommunikationsgerät (10) und einem zweiten Telekommunikationsgerät (18) eines Telekommunikationsnetzwerkes (14), dadurch gekennzeichnet,

dass ein Zentralmodul vorausbezahlte Zugangsdaten erzeugt, wobei die vorausbezahlten Zugangsdaten einen ersten digitalen Schlüssel und Kontrolldaten umfassen, und wobei die vorausbezahlten Zugangsdaten in einem Speichermodul (11) des ersten Telekommunikationsgeräts (10) abgespeichert werden,

dass das Zentralmodul einen dem ersten digitalen Schlüssel zugeordneten zweiten digitalen Schlüssel erzeugt, wobei der zweite digitale Schlüssel auf einer oder mehreren Steuereinheiten (16) des Telekommunikationsnetzwerks (14) abgespeichert wird,

dass das erste Telekommunikationsgerät (10) basierend auf Kontrolldaten der vorausbezahlten Zugangsdaten ein Gültigkeitskriterium ermittelt und Nutzdaten des ersten Telekommunikationsgeräts mittels des ersten Schlüssels codiert, solange das Gültigkeitskriterium erfüllt ist, und

dass das erste Telekommunikationsgerät (10) codierte Nutzdaten an die Steuereinheit (16) übermittelt, wobei die Steuereinheit (16) mittels des zweiten digitalen Schlüssels überprüft, dass die codierten Nutzdaten mit dem ersten digitalen Schlüssel codiert sind, wobei die Steuereinheit (16) bei einer erfolgreichen Überprüfung die codierten Nutzdaten decodiert, und wobei die Steuereinheit (16) die decodierten Nutzdaten an das zweite Telekommunikationsgerät (18) übermittelt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die im Speichermodul (11) des ersten Telekommunikationsgeräts (10) abgespeicherten vorausbezahlten Zugangsdaten bei der Codierung von Nutzdaten modifiziert und/oder gelöscht werden.

3. Verfahren nach einem der Ansprüche 1 bis 2, dadurch gekennzeichnet, dass die im Speichermodul (11) des ersten Telekommunikationsgeräts (10) abgespeicherten vorausbezahlten Zugangsdaten einen Geldbetragswert umfassen, wobei dieser Geldbetragswert bei der Codierung von Nutzdaten modifiziert und/oder gelöscht wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die vorausbezahlten Zugangsdaten auf einem SIM-Modul (12) des ersten Telekommunikationsgeräts abgespeichert werden.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Codierung der Nutzdaten eine digitale Verschlüsselung und/oder digitale Signierung umfasst und dass die Decodierung der Nutzdaten eine entsprechende digitale Entschlüsselung und/oder Verifikation einer digitalen Signatur umfasst.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die vorausbezahlten Zugangsdaten eine Berechtigung für die Codierung einer bestimmbaren Nutzdatenmenge umfassen, wobei die vorausbezahlten Zugangsdaten gelöscht werden, sobald die Codierung der bestimmbaren Nutzdatenmenge abgeschlossen ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass mehrere Blöcke mit vorausbezahlten Zugangsdaten im Speichermodul (11) des ersten Telekommunikationsgeräts (10) abspeicherbar sind.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Kontrolldaten mehrere Blöcke umfassen, wobei für jeden Block die Ermittlung eines Gültigkeitskriteriums sowie die Modifikation oder Löschung des entsprechenden Blocks von Kontrolldaten durchführbar ist.

9. System zur Ausführung des Verfahrens nach einem der Ansprüche 1 bis 8, mit einem ersten Telekommunikationsgerät (10), welches ein SIM-Modul (12) umfasst, mit einem MSC (Mobile Switching Center) (16), das mit

dem ersten Telekommunikationsgerät (10) über ein Telekommunikationsnetzwerk (14) verbindbar ist, dadurch gekennzeichnet,

dass mittels eines Zentralmoduls vorausbezahlte Zugangsdaten mit einem ersten digitalen Schlüssel und mit Kontrolldaten sowie ein entsprechender zweiter digitaler Schlüssel erzeugbar sind,

dass vorausbezahlten Zugangsdaten auf dem in einem Speichermodul (11) des SIM-Moduls (12) des ersten Telekommunikationsgeräts (10) abspeicherbar sind,

dass der zweite digitale Schlüssel in einem Speichermodul (24) des MSC (16) abspeicherbar ist,

dass mittels des ersten Telekommunikationsgeräts (10) und im Speichermodul (11) abgespeicherter vorausbezahlter Zugangsdaten Gültigkeitskriterien überprüfbar und Nutzdaten des ersten Telekommunikationsgeräts (10) codierbar sind, und

dass mittels des MSC (16) und dem im Speichermodul (24) abgespeicherten zweiten digitalen Schlüssel codierte Nutzdaten des ersten Telekommunikationsgeräts (10) decodierbar sind und die decodierten Nutzdaten an ein zweites Telekommunikationsgerät (18) übermittelbar sind.

10. System nach Anspruch 9, dadurch gekennzeichnet, dass das erste Telekommunikationsgerät (11) ein Verschlüsselungsmodul oder ein Signierungsmodul zur Verschlüsselung oder Signierung von Nutzdaten mittels des ersten digitalen Schlüssels umfasst, und dass das MSC (16) ein Entschlüsselungsmodul oder ein Signaturverifikationsmodul zur Entschlüsselung oder Verifikation der Signatur von verschlüsselten oder signierten Nutzdaten mittels des zweiten digitalen Schlüssels umfasst.

FIG. 1

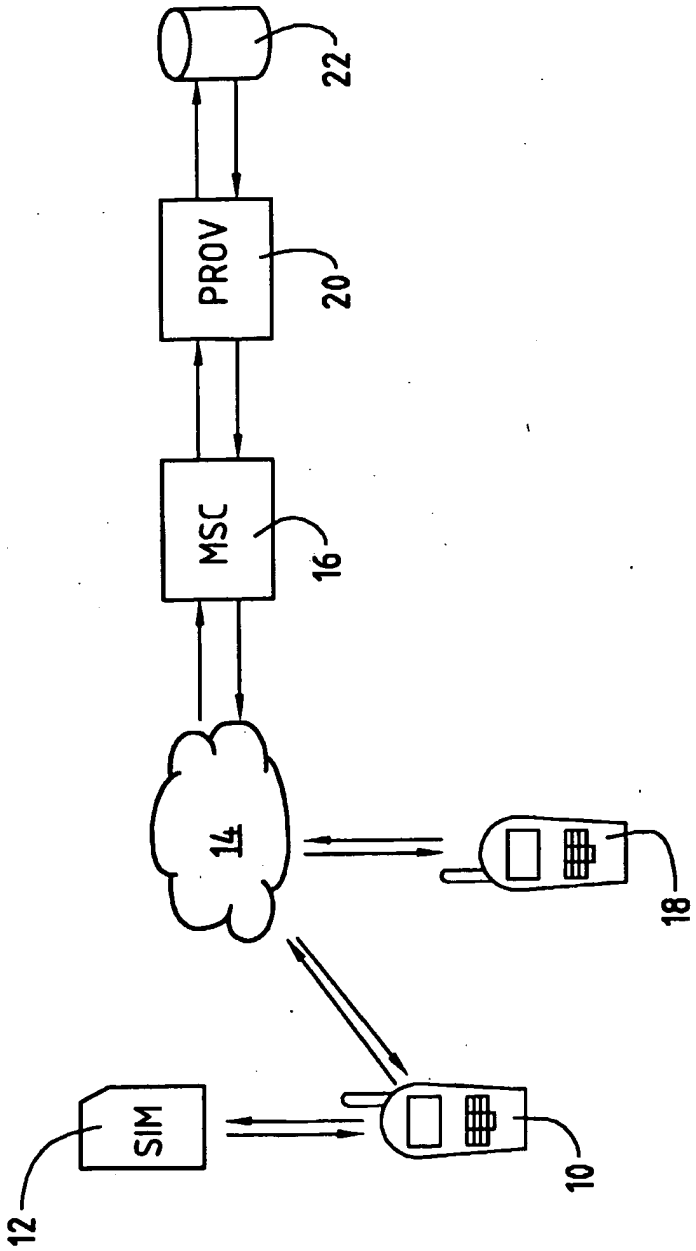


FIG. 2